COUNTING SEMILINEAR ENDOMORPHISMS OVER FINITE FIELDS

TIM HOLLAND

1. Introduction

Fix a prime p and finite field k of order $q := p^r$. For a field automorphism τ of k and a k-vector space V of dimension g, we will write $\mathrm{End}^\tau(V)$ for the set of *τ-semilinear endomorphisms of V*; that is, additive maps $F : V \to V$ which satisfy $F(\alpha v) = \tau(\alpha) \cdot F(v)$ for all $v \in V$ and $\alpha \in k$. As τ is an automorphism, the kernel and image (as sets, say) of any τ-semilinear map F are both k-subspaces of V, and this gives a well-defined notion of rank and nullity. Moreover, one has a canonical direct sum decomposition $V \simeq V^{F-\mathrm{bij}} \oplus V^{F-\mathrm{nil}}$ where $V^{F-\mathrm{bij}}$ is the maximal subspace of V on which F is bijective, so we may speak of the "infinity rank" of F, which by definition is $\mathrm{rk}_\infty(F) := \dim_k(V^{F-\mathrm{bij}})$. For any pair of nonnegative integers r, s satisfying $s \le r \le g$, we may thus define the set

$$P^\tau_{r,s} := \{F \in \mathrm{End}^\tau(V) \ : \ \mathrm{rk}(F) = r \text{ and } \mathrm{rk}_\infty(F) = s\}. \tag{1.1}$$

These sets show up naturally in the classification of finite flat p-power order group schemes over k which are killed by p and which have p-rank s, via Dieudonné theory. It is therefore natural to ask for a closed formula (in $q = \#k$) for the cardinality of $P^\tau_{r,s}$, and the main result of this paper is precisely such a formula:

Theorem 1.1. *Let g be a positive integer and r, s nonnegative integers with $s \le r \le g$. For any fixed automorphism τ of k and any g-dimensional vector space V, the number of τ-semilinear endomorphisms of V with rank r and infinity rank s is*

$$\#P^\tau_{r,s} = \frac{q^{g^2}}{q^{(g-r)^2+r-s}} \frac{\displaystyle\prod_{j=1}^{g}(1-q^{-j}) \prod_{j=g-r}^{g-s-1}(1-q^{-j})}{\displaystyle\prod_{j=1}^{r-s}(1-q^{-j}) \prod_{j=1}^{g-r}(1-q^{-j})}$$

Here, we follow the usual convention that a product indexed by the empty set takes the value 1. Note that $P^{\mathrm{id}}_{g,g}$ is identified with $\mathrm{GL}_g(k)$ upon choosing a basis of V, while the union of $P^{\mathrm{id}}_{r,0}$ for $0 \le r \le g$ is, upon choosing a basis of V, the set of nilpotent $g \times g$ matrices with entries in k, so our formula may be used to recover the well-known formulae for the order of $\mathrm{GL}_g(k)$ and for the number of nilpotent $g \times g$ matrices over k (for which, see [2]). In fact, our argument is a natural generalization of the proof of the main result of [2], though some care is required in our method to deal with the issue of semilinearity. We remark that Theorem 1.1 provides key input for one of the main results of [1], and indeed this was the genesis of the present note.

Date: December 22, 2011.

2010 *Mathematics Subject Classification.* 15A04 (15A03 15A33).

The author is grateful to David Zureick-Brown for sharing his ideas and to Bryden Cais and Jeremy Booher for supervising his 2011 PROMYS research project.

2. Flags and adapted bases

In this section, we summarize the concepts and tools from semilinear algebra that will figure in the proof of Theorem 1.1. We keep the notation of §1; in particular, a g-dimensional k-vector space V.

We begin by noting that for an automorphism τ of k, the set $\mathrm{End}^{\tau}(V)$ is naturally a k-vector space, and that for $F \in \mathrm{End}^{\tau}(V)$ and $F' \in \mathrm{End}^{\tau'}(V)$, the composition $F \circ F'$ lies in $\mathrm{End}^{\tau\circ\tau'}(V)$. For $F \in \mathrm{End}^{\tau}(V)$, one checks that the subsets $\ker(F)$ and $\mathrm{im}(F)$, defined in the usual way, are actually k-linear subspaces of V, and we set $\mathrm{rk}(F) := \dim_k(\mathrm{im}(F))$. By definition, the *terminal image* of F is the subspace

$$V^{F-\mathrm{bij}} := \bigcap_{n\geq 0} \mathrm{im}(F^n),$$

and we define the infinity rank of F to be the dimension of its terminal image: $\mathrm{rk}_{\infty}(F) := \dim_k V^{F-\mathrm{bij}}$. An easy argument shows that in fact $\mathrm{rk}_{\infty}(F) = \mathrm{rk}(F^g)$, and that F is bijective on $V^{F-\mathrm{bij}}$, which justifies the notation. In fact, $V^{F-\mathrm{bij}}$ is the maximal F-stable subspace of V on which F is bijective [].

Definition 2.1. Let r be a nonnegative integer and

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_{r-1} \supsetneq V_r = 0 \tag{2.1}$$

be a flag in V. Set $d_i = \dim V_i$. We say that an ordered basis $\{v_1, v_2, \ldots, v_g\}$ of V is *adapted* to the given flag (2.1) if $\{v_{g-d_i+1}, \ldots, v_n\}$ is a basis of V_i for all i.

Given a flag in V and a fixed ordered basis $\mathbf{e} := \{e_i\}_{1\leq i\leq g}$ of V, there is a canonical procedure from the theory of Schubert cells which associates to $\mathbf{e}$ an adapted basis of the given flag, which we now explain.

First, suppose that U is an arbitrary subspace of V, and for $1 \leq j \leq g$ define

$$U_j := U \cap \mathrm{span}\{e_{j+1}, e_{j+2}, \ldots, e_g\},$$

with the convention that $U_g = 0$. We then have descending chain of subspaces

$$U = U_0 \supseteq U_1 \supseteq \cdots \supseteq U_g = 0$$

with the property that $\dim(U_{j-1}) - \dim(U_j) \leq 1$ and equality holds if and only if $U_{j-1} \neq U_j$. We define

$$J := \{j \ : \ U_{j-1} \neq U_j\}$$

and put $m := \#J$; note that this integer is equal to the dimension of U.

Lemma 2.2. *For each $j \in J$, there is a unique vector $u_j \in U_{j-1}$ with*

$$u_j - e_j \in \mathrm{span}\{e_i \ : \ i > j,\ i \notin J\}.$$

Moreover, $\{u_j \ : \ j \in J\}$ is a basis of U, and if the last n-vectors of $\mathbf{e}$ lie in U for some $n \leq m$, then $u_j = e_j$ for all $j \in J$ with $j \geq g - n + 1$.

Proof. We list the m elements of J in increasing order $j_1 < j_2 < \cdots < j_m$. By definition of J, the complement of U_{j_i} in U_{j_i-1} is 1-dimensional for $1 \leq i \leq m$, so we may pick a nonzero vector v_{j_i} in this complement which spans it. Then v_{j_m} is a linear combination of $\{e_i \ : \ i \geq j_m\}$ with a nonzero coefficient of e_{j_m} by construction. We may therefore uniquely scale v_{j_m} by the inverse of this coefficient to obtain a vector $u_{j_m} \in U_{j_m}$ which satisfies (2.2). Now suppose inductively that

vectors $u_{j_m}, u_{j_{m-1}}, \ldots, u_{j_{d+1}}$ satisfying the condition of the Lemma have been uniquely determined. We may uniquely write our choice v_{j_d} as

$$v_{j_d} = c_0 e_{j_d} + \sum_{i=1}^{g-j_d} c_i e_{j_d+i}$$

with c_0 necessarily nonzero. We then define

$$u_{j_d} = c_0^{-1} v_{j_d} - \sum_{\substack{j_d+i \in J \\ 1 \le i \le g-j_d}} c_0^{-1} c_i e_{j_d+i}$$

One checks that u_{j_d} satisfies (2.2). Multiplying our choice v_{j_d} by any nonzero scalar gives the same vector u_{j_d}; in particular, the u_{j_i} are independent of our initial choices of the v_{j_i} and so are uniquely determined. That the set $\{u_j : j \in J\}$ is a basis of U follows immediately from our construction, as does the fact that $u_j = e_j$ for $j \ge g-n+1$ when the last n vectors of the ordered basis $\mathbf{e}$ lie in U. □

For a fixed ordered basis $\mathbf{e} = \{e_i\}$ of V and a subspace U of V, the procedure of Lemma 2.2 yields, in a canonical way, a new ordered basis $\{e_j : j \notin J\} \cup \{u_j : j \in J\}$ of V with the property that the final m vectors are a basis of U. We will say that this process *adapts* the basis $\mathbf{e}$ to the subspace U. Note that the process of adapting an ordered basis to U does not change the final n vectors when these vectors lie in U.

Given a flag (2.1) in V and a fixed ordered basis $\mathbf{e}$ of V, we now associate a canonical adapted basis $\mathbf{v}$ as follows. First, we adapt $\mathbf{e}_r := \mathbf{e}$ to V_{r-1} to obtain a new ordered basis $\mathbf{e}_{r-1}$ of V with the property that the last d_{r-1} vectors are a basis of V_{r-1}. We then adapt $\mathbf{e}_{r-1}$ to V_{r-2} to obtain a new ordered basis of V in which the last d_{r-2} vectors are a basis of V_{r-2} and the last d_{r-1} vectors are a basis of V_{r-1} (as $V_{r-1} \subseteq V_{r-2}$ so the last d_{r-1} vectors of $\mathbf{e}_{r-2}$ and $\mathbf{e}_{r-1}$ coincide as we have noted). We continue in this manner, until we arrive at the adapted basis $\mathbf{v} := \mathbf{e}_1$; by the unicity of Lemma 2.2, this $\mathbf{v}$ is uniquely determined by the flag 2.1 and the fixed ordered basis $\mathbf{e}$ of V.

3. Proof of Theorem 1.1

Our proof of Theorem 1.1 will proceed in two steps. First, using flags and adapted bases, we will show that the set $P^{\tau}_{r,s}$ defined by (1.1) is in bijection with a certain set consisting of lists of vectors; we will then count this latter set.

Definition 3.1. For r, s nonnegative integers with $s \le r \le g$, we define $X_{r,s}$ to be the subset of V^g consisting of all g-tuples $(x_1, x_2, \ldots, x_g)$ which satisfy:

(1) $\dim \operatorname{span}\{x_j\}_{j=1}^{g} = r$
(2) $\dim \operatorname{span}\{x_j\}_{j=g-s+1}^{g} = s$
(3) $x_{g-s} \in \operatorname{span}\{x_j\}_{j=g-s+1}^{g}$.

Now let τ be any automorphism of k and fix, once and for all, a choice $\mathbf{e}$ of k-basis of V. Any $F \in P^{\tau}_{r,s}$ determines a flag in V via $V_i := F^i(V)$, and this flag necessarily has the form

$$V = V_0 \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_t = V_{t+1} = V_{t+2} \cdots \tag{3.1}$$

with $V_1 = \operatorname{im}(F)$ of dimension r and V_t of dimension s (as it is the terminal image of F). Adapting $\mathbf{e}$ to (3.1) as in §2.2 uniquely determines an ordered basis $\mathbf{v}_F := \{v_{F,i}\}_{i=1}^{g}$ of V (that depends on F), and we define a map of sets

$$\mu : P^{\tau}_{r,s} \longrightarrow V^g \qquad \text{by} \qquad \mu(F) := (F(v_{F,1}), F(v_{F,2}), \ldots, F(v_{F,g})). \tag{3.2}$$

The following Lemma is key:

Lemma 3.2. *The map μ of (3.2) is a bijection onto $X_{r,s}$.*

Proof. It is clear from our construction that μ has image contained in $X_{r,s}$, so it suffices to construct an inverse mapping which we do as follows. Given an arbitrary element $x := (x_i)_{i=1}^{g}$ of $X_{r,s}$, we set $V_0 := V$ and $d_0 := g$ and for $i \geq 1$ inductively construct a flag in V by defining

$$V_i := \operatorname{span}\{x_{g-d_{i-1},\ldots,x_g}\} \qquad \text{and} \qquad d_i := \dim(V_i). \tag{3.3}$$

Letting $\mathbf{v}_x = \{v_{x,i}\}_{i=1}^{g}$ be the adaptation of the basis $\mathbf{e}$ to this flag, we define $F_x \in \operatorname{End}^{\tau}(V)$ to be the unique τ-semilinear endomorphism of V satisfying $F_x(v_{x,i}) = x_i$ for all i. That is, for arbitrary $v \in V$, we write $v = \sum c_i v_{x,i}$ as a unique linear combination of the basis vectors $v_{x,i}$ and we define $F_x(v) := \sum \tau(c_i)x_i$, which is visibly a τ-semilinear endomorphism of V. We claim that $V_i = F_x^i(V)$ for all i. For $i = 0$ this is simply the definition of $V_0 = V$. Inductively supposing that $F_x^i(V) = V_i$ for some $i \geq 0$, we then have

$$\begin{aligned} F_x^{i+1}(V) = F_x(F_x^i(V)) = F_x(V_i) &= F_x(\operatorname{span}\{v_{x,j}\}_{j=g-d_i+1}^{g}) \\ &= \operatorname{span}\{F_x(v_{x,j})\}_{j=g-d_i+1}^{g} \\ &= \operatorname{span}\{x_j\}_{j=g-d_i+1}^{g} \\ &= V_{i+1}, \end{aligned}$$

where in the final equality on the first line we have use the fact that the last d_i vectors in the adapted basis $\mathbf{v}_x$ span V_i by construction. We conclude from the definition of $X_{r,s}$ that F_x lies in $P_{r,s}^{\tau}$, and we define $\nu : X_{r,s} \to P_{r,s}(V)$ to be the map of sets which sends x to F_x. It is a then straightforward exercise to check that ν and μ are inverse mappings of sets. ☐

We now wish to enumerate the set $X_{r,s}$. We remark that the set $X_{r,s}$ is independent of τ, so that the semilinearity aspect of our counting problem has been entirely removed at this point. The s vectors $x_{g-s+1}, \ldots, x_g$ of V must be linearly independent, but otherwise may be chosen arbitrarily from V; in particular, there are

$$\prod_{i=0}^{s-1}(q^g - q^i) \tag{3.4}$$

ways to do this. Supposing that $x_{g-s+1}, \ldots, x_g$ have been chosen, we write V_∞ for their span and we put $n := g - s$ and $d := r - s$. A choice $x_1, \ldots, x_n$ of n-vectors in V will have the property that the g-vectors $x_1, \ldots, x_g$ span an r-dimensional subspace of V if and only if the images of $x_1, \ldots, x_n$ span a d-dimensional subspace of $W := V/V_\infty$. The condition (3) in the definition of $X_{r,s}$ (Definition 3.1) that x_{g-s} lie in V_∞ is of course equivalent to the condition that its image in W be zero. We are therefore reduced to computing the cardinality of the set

$$Q_{n,d} := \{(w_i)_{i=1}^{n-1} \in W^{n-1} \ : \ \dim \operatorname{span}\{w_i\}_{i=1}^{n-1} = d\}.$$

As usual, we write $\operatorname{Gr}(W, d)$ for the Grassmannian of d-dimensional subspaces of W and for any k-vector space U, we denote by $\operatorname{Hom}_k^{\text{surj}}(k^{n-1}, U)$ the set of k-linear surjective homomorphisms from k^{n-1} onto U. We then define the set

$$A_{n,d} := \{(U, T) \ : \ U \in \operatorname{Gr}(W, d) \text{ and } T \in \operatorname{Hom}_k^{\text{surj}}(k^{n-1}, U)\}$$

as well as a map of sets

$$\gamma : Q_{n,d} \longrightarrow A_{n,d} \qquad \text{by} \qquad \gamma((w_i)_{i=1}^{n-1}) := (\operatorname{span}\{w_i\}_{i=1}^{n-1},\ T : \sum c_i f_i \mapsto \sum c_i w_i) \tag{3.5}$$

where $\{f_i\}_{i=1}^{n-1}$ is the standard basis of k^{n-1}.

Lemma 3.3. *The map γ of (3.5) is bijective.*

Proof. The map $\delta : A_{n,d} \to Q_{n,d}$ sending (U,T) to $\{Tf_i\}_{i=1}^{n-1}$ is clearly inverse to γ. □

To count $Q_{n,d}$, it therefore suffices to count $A_{n,d}$. To do this, we note that for any d-dimensional k-vector space U, choosing a basis of U gives a bijection between the set $\mathrm{Hom}_k^{\mathrm{surj}}(k^{n-1}, U)$ and the set of $(n-1) \times d$ matrices over k with rank d, and we deduce that

$$\# \mathrm{Hom}_k^{\mathrm{surj}}(k^{n-1}, U) = \prod_{i=0}^{d-1} (q^{n-1} - q^i) \tag{3.6}$$

for any such U (note, in particular, that this is independent of U). As the count

$$\# \mathrm{Gr}(W, d) = \frac{\prod_{i=0}^{d-1} (q^n - q^i)}{\prod_{i=0}^{d-1} (q^d - q^i)} \tag{3.7}$$

is standard, we conclude from (3.7), (3.6) and Lemma 3.3 that

$$\# Q_{n,d} = \# \mathrm{Gr}(W,d) \cdot \# \mathrm{Hom}_k^{\mathrm{surj}}(k^{n-1}, U) = \frac{\prod_{i=0}^{d-1} (q^n - q^i)}{\prod_{i=0}^{d-1} (q^d - q^i)} \prod_{i=0}^{d-1} (q^{n-1} - q^i). \tag{3.8}$$

For each $w \in W = V/V_\infty$, there are $\# V_\infty = q^s$ ways to lift w to a vector in V, and hence $q^{sn} = q^{s(g-s)}$ ways to lift any list of $n = g - s$ vectors in W to V. Thus, by (3.8), the number of choices for the first $g - s$ vectors $(x_i)_{i=1}^{g-s}$ is

$$q^{s(g-s)} \frac{\prod_{i=0}^{r-s-1} (q^{g-s} - q^i)}{\prod_{i=0}^{r-s-1} (q^{r-s} - q^i)} \prod_{i=0}^{r-s-1} (q^{g-s-1} - q^i). \tag{3.9}$$

Combining (3.9) and (3.4) and using Lemma 3.2 then gives

$$\# P_{r,s}^{\tau} = \# X_{r,s} = q^{s(g-s)} \frac{\prod_{i=0}^{r-s-1} (q^{g-s} - q^i)}{\prod_{i=0}^{r-s-1} (q^{r-s} - q^i)} \prod_{i=0}^{r-s-1} (q^{g-s-1} - q^i) \prod_{i=0}^{s-1} (q^g - q^i), \tag{3.10}$$

which, after some elementary algebraic manipulation, is readily seen to be equivalent to the formula of Theorem 1.1.

References

[1] B. R. Cais, J. S. Ellenberg, and D. M. Zureick-Brown. Random dieudonné modules, random p-divisible groups, and random curves over finite fields. *Preprint*, 2012.

[2] M. C. Crabb. Counting nilpotent endomorphisms. *Finite Fields Appl.*, 12(1):151–154, 2006.